Steganographie

- [Exploitation/Stegano] StegHide
- [Exploitation/Stegano] Stegseek
- [Exploitation/Stegano] Strings
- [Exploitation/Stegano] Exiftool
- [Exploitation/Stegano] Aperi'Solve
- [Exploitation/Stegano] PixRecovery & GHex

[Exploitation/Stegano] StegHide

Introduction

L'outil **steghide** permet de cacher des fichiers dans d'autres fichiers (généralement des images) en définissant un mot de passe pour accéder à ce fichier caché.

Une fois le fichier B caché dans le fichier A, si quelqu'un parvient à récupérer le fichier A et la passphrase il pourra récupérer le fichier B en utilisant steghide.

Installation

```
sudo apt install steghide
```

Manuel

Syntaxe générale

```
steghide [embed|extract|info] [OPTIONS]
```

Cacher un fichier B dans un fichier A

```
steghide embed -cf <FILE_A> -ef <FILE_B>
```

> Une passphrase vous sera demandée !

Extraire un fichier B du fichier A

```
steghide extract -sf <FILE_A>
```

> La passphrase vous sera demandée !

[Exploitation/Stegano] Stegseek

Introduction

L'outil **stegseek** permet de lancer des attaque **bruteforce** sur les passphrases des fichiers cachés par steghide dans d'autres fichiers.

Steghide permet par défaut de le faire mais la tâche est complexe est lente.

Source

- Github du projet

Installation

```
wget https://github.com/RickdeJager/stegseek/releases/download/v0.6/stegseek_0.6-1.deb && sudo apt install -y ./stegseek_0.6-1.deb && rm -f stegseek_0.6-1.deb
```

Manuel

Attaque brute force

```
stegseek <STEGANO_FILE> <WORDLIST>
```

Récupération de meta-donnée non chiffrée

Les meta-données non-chiffrées de steghide sont protégées par une **seed** codée d'une longueur de **2^32** (cassable en quelques minutes maxium).

L'outil va donc récupérer les méta-données pour essayer de récupérer :

- Si le fichier contient vraiment de la donnée ajoutée par steghide.
- La quantitié de donnée.
- L'algorithme de chiffrement.
- Si aucun chiffrement n'est présent, le contenu sera affiché.

Voici la commande à effectuer pour lancer la récupération d'informations :

```
stegseek --seed [STEGANO_FILE]
```

[Exploitation/Stegano] Strings

Introduction

Bien que la commande **strings** sur Linux ne servent pas qu'à la stéganographie, elle est très pratique dans ce cas d'usage pour extraire toutes les chaînes de caractères contenues dans un fichier et ainsi, récupérer de la donnée cachée.

Manuel

```
strings <FILE>
```

[Exploitation/Stegano] Exiftool

Introduction

En stéganographie et en énumération, il peut être intéressant d'obtenir les méta-données contenues dans un fichier puisqu'elles peuvent regorger d'informations utiles.

C'est là qu'entre en jeu l'outil **exiftool** qui permet d'afficher ces méta-données.

Manuel

Affichage des méta-données

```
exiftool <FILE>
```

Affichage de toutes les informations disponibles

```
exiftool -a -u <FILE>
```

[Exploitation/Stegano] Aperi'Solve

Introduction

Ce site web regroupe tout un tas de test pour la stéganographie.

Site

https://www.aperisolve.com/

[Exploitation/Stegano] PixRecovery & GHex

Introduction

Ces outils permettent de réparer des images corrompus.

PixRecovery

https://online.officerecovery.com/fr/pixrecovery/

GHex

Cet outil graphique est une alternative à l'outil en ligne de commande **hexedit**.

Il permet d'éditer l'héxadécimal d'un fichier ce qui peut servir pour changer le **magic byte** d'un fichier corrompu et le rendre fonctionnel dans certains cas.

Voici la page wikipédia qui répertorie les magic bytes de diférents types de fichiers :

https://en.wikipedia.org/wiki/List_of_file_signatures